Steven A. Christensen (USB 5190)
Christensen Young & Associates, PLLC
9980 South 300 West #200
Sandy, UT 84070
Telephone: (801) 676-6447
Facsimile: (888) 569-2786
steven@christensenyounglaw.com

IN THE UNITED STATES DISTRICT COURT DISTRICT OF UTAH, CENTRAL DIVISION	
Tom Partridge, Zane L. Christensen, Jennifer J. Christensen, Zachary A. Christensen, Cameron Christensen, e*t al* and unknown Plaintiffs 1-143,000,000 Plaintiffs v. Equifax, Incorporated, Equifax Information Services, LLC and Does 1-1,000	CLASS ACTION COMPLAINT Case No: 2:17-cv-01017 DBP Judge Dustin B. Pead

COME NOW Plaintiffs, individually and on behalf of the classes defined below, bring this Class Action Complaint ("Complaint") against Equifax, Inc., and allege as follows:

NATURE OF THE CASE

1. On September 7, 2017 Plaintiffs were advised that Equifax, Inc., and Equifax Information Services, LLC (hereinafter jointly referred to as "Equifax") were the subject of a data breach, in which unauthorized individuals accessed Equifax's website ("Data Breach"). Plaintiffs believe the unauthorized individuals who accessed the website have already used information gained in the breach, including names, addresses, Social Security numbers, alternative identification numbers, driver's license information, wage information, employment information, and other personal information, to sell and compromise Plaintiffs' information.

2. Equifax was aware of the Data Breach in July of 2017, but refused to comment on the Data Breach, or provide any notification directly to affected individuals at that time, and it was not until September 7, 2017 that the information became public.

3. The Data Breach occurred because Equifax failed to implement adequate security measures to safeguarded consumers' Personal Identifying Information ("PII") and willfully ignored known weaknesses in its data security, including prior hacks into its information

systems. Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems—especially from entities such as Equifax, which are known to possess a large number of individuals' valuable personal and financial information.

4. Armed with this personal information, identity thieves can commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, purchase cars, and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in a victim's name; obtain medical services in a victim's name; or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other individuals who intend to misuse the information.

5. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiff and Class Members have been exposed to fraud, identity theft, and financial harm, as detailed below, and to a substantial, heightened, and imminent risk of such harm in the future. It cannot be questioned that the PII of Plaintiffs and Class Members was taken for the purpose of stealing the identity of Plaintiffs and Class Members which has already resulted in and will continue to result in damage to them. Plaintiffs and Class Members have to monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur, additional out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the Data Breach's impact on their PII for the remainder of their lives. Going forward, Plaintiffs and Class Members anticipate spending considerable time and money for the rest of their lives in order to detect and respond to the impact of the Data Breach.

6. There is a substantial likelihood that Class Members already have or will become victims of identity fraud given the breadth of information about them that is now publicly available. Javelin Strategy & Research reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud...- "In fact, [i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud."" Javelin also found increased

instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal."

7. As described by former Equifax Vice President of identity and fraud product management , Gasan Awad, "Data breaches are the first step for criminals with intentions to steal and misuse consumer information. Once fraudsters have consumers' private identity information they then take the next step in criminal activity, often committing fraud by opening fraudulent accounts or taking over an existing account. In essence, fraudsters use the personal information obtained from the breaches to apply for credit or benefits or hijack existing accounts, all while acting as the victims."[1]

8 Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs seek to recover damages, including actual and statutory damages, equitable relief, reimbursement of out-of-pocket losses, other compensatory damages, credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

9. Rick Smith, Chairman and CEO of Equifax, announced on September 7, 2017 that Equifax experienced a Data Breach impacting approximately 143 million U.S. consumers. The Data Breach occurred from mid-May through July 2017.[2]

PARTIES

10. Plaintiffs Tom Partridge, Zane and Jennifer Christensen are residents of South Jordan, Utah, Zachary Christensen is a resident of Sandy, Utah, and Cameron Christensen is a resident of Lehi, and all Plaintiffs were citizens of the United States during the period of the Data Breach. Plaintiffs were not notified by Equifax of the Data Breach, and as a result of the Data Breach run the substantial risk of identity theft.

---

[1] Awad, Gasan, Device Advice: Keeping Fraudsters from Consumer Info, http://www.darkreading.com/endpoint/device-advice-keeping-fraudsters-from-consumer-info/a/d- d/1325182

[2] https://www.equifaxsecurity2017.com The CEO additionally noted that the Social Security numbers, birth dates, addresses and driver's license numbers were effected. Additionally, credit card numbers of approximately 209,000 U.S. consumers, along with over 182,000 dispute documents containing personal identifying information was taken.

11. Defendant Equifax, Inc. is incorporated in Georgia with its headquarters and principal place of business located at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309, and conducts business in all 50 States.

12. Equifax is one of the three major credit reporting agencies in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, as described by Equifax "[t]he company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers."[3] As a credit bureau service, Equifax maintains information related to the credit history of consumers and provides the information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different from Defendant.

14. This Court has personal jurisdiction over Defendant because it conducts business in the State of Utah, and maintains sufficient minimum contacts in Utah, intentionally availing itself of this jurisdiction by conducting operations in Utah.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Equifax regularly transacts business in this District, and Plaintiffs claims occurred in this District.

FACTS

16 On September 7, 2017 Equifax announced that it had been subject to the Data Breach, and that 143 million accounts had been compromised by unauthorized persons. The PII in Equifax's files includes, but is not limited to; names, addresses, Social Security numbers, alternative identification numbers, driver's license information, wage information, employment information, and other personal information.

[3] http://www.equifax.com/about-equifax/company-profile

17. Defendant Equifax failed to acknowledge, or notify the victims of the Data Breach for over six weeks after it learned of the Data Breach.

18. According to an Equifax spokesperson, the Equifax services which were the subject of the Data Breach, were normal Equifax operating procedures.

19. Equifax, as a credit bureau service, is engaged in a number of credit-related services, including providing services through The Work Number®, the most extensive source of income and employment information in the United States. Individuals obtain credit and other benefits through the verifications of income and employment Equifax provides to lenders, social service agencies and others pursuant to an individual's authorization." [4] As described by Equifax, "[b]usinesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, debt management and human resources-related services. We also offer products that enable individual consumers to manage their financial affairs and protect their identity."[5]

20. Prior to the Data Breach, Equifax promised its customers, and everyone about whom it collects PII, that it would reasonably protect their PII. Equifax's privacy policy stated, in relevant part: "We are committed to protecting the security of your information through procedures and technology designed for this purpose."[6]

21. Equifax further cautioned small businesses utilizing its services to "[c]hoose your passwords carefully: ...Don't use your name, address, phone number, initials, Social Security number, license plate or birthday..."[7]

22. Plaintiffs and Class Members' PII information was disclosed to Equifax, and Equifax compiled, maintained, and furnished Class Members' PII, to third parties. Equifax is allowed to perform such services, involving such sensitive information, only if it adheres to the requirements of laws meant to protect the privacy of such information, such as the Gramm-Leach-Bliley Act ("GLBA"). Equifax's maintenance, use, and furnishing of such PII is, and

[4] http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/
[5] 2016 Equifax Annual Report, pg. 12, http://www.equifax.com/assets/corp/2016_annual_report.pdf
[6] http://www.equifax.com/privacy/about-equifax-corporation#EffortsWeMakeToSafeguardYourPersonalInformation
[7] http://www.equifax.com/privacy/equifax-small-business

was, intended to affect Plaintiffs and other Class Members, and the harm caused by disclosure of that PII in the Data Breach was entirely foreseeable to Equifax.

23. Equifax touts itself as an industry leader in data breach security and often promotes the importance of data breach prevention. Equifax offers services directly targeted to assisting businesses who have encountered a data breach.[8]

24. Equifax expressly advises businesses which have lost customer data to "Quickly Notify Those Affected;" "Provide Personalized Communication;" and "Offer Credit Protection."[9] Despite those admonitions, to date, Equifax has not reached out to affected individuals, and has not provided personalized communications to those affected, or offered credit protection to those whose PII was compromised by the Data Breach.

25. Since identity thieves use the PII of other people to commit fraud or other crimes, Plaintiffs and other consumers whose information was exposed in the Data Breach are subject to a substantial, increased, concrete risk of identity theft. Javelin Strategy & Research also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal."[10]

26. The exposure of Plaintiff s and Class Members' Social Security numbers, in particular, poses serious problems. Criminals frequently use Social Security numbers to create false bank accounts, file fraudulent tax returns, and incur credit in the victim's name. Neal O'Farrell, a security and identity theft expert for Credit Sesame calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."[11] Even where data breach victims obtain a new Social Security number, the Social Security Administration warns "that a new number probably will not solve all problems... and will not guarantee [] a fresh start."[12] In fact, "[f]or some victims of identity theft, a new number actually creates new problems." One of those new problems is that a new Social Security number will have a completely blank credit history,

[8] http://www.equifax.com/business/equifax-breach-products
[9] *Id.*
[10] https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy
[11] http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html
[12] https://www.ssa.gov/pubs/EN-05-10064.pdf

making it difficult to get credit for a few years unless it is linked to the old, compromised number.

27. As a result of the compromising of their personal information, Plaintiffs and Class Members have experienced and will face a substantial risk of experiencing, *inter alia*, the following injuries:

- money and time expended to prevent, monitor, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- costs of credit monitoring, as Defendant has offered none to date;
- costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking full reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;
- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;
- loss of the opportunity to control how their personal information is used; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

28. The risks that Plaintiffs and Class Members bear as a result of the Data Breach cannot be fully mitigated by credit monitoring because it can only help detect, but will not prevent, the fraudulent use of Plaintiff s and Class Members' PII. Instead, Plaintiffs and Class Members will need to spend time and money to protect themselves. For instance, credit reporting agencies impose fees for credit freezes in certain states. In addition, while credit reporting agencies offer consumers one free credit report per year, consumers who request more than one credit report per year from the same credit reporting agency (such as Equifax) must pay a fee for the additional report. Such fees constitute out-of-pocket costs to Plaintiffs and Class Members.

29. Equifax is a "financial institution" pursuant to the Gramm-Leach-Bliley Act ("GLBA"), and as such GLBA imposes "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801 (b)

30. Credit bureaus are "financial institutions" for purposes of the GLBA, and are therefore subject to its provisions. *See TransUnion LLC v. F.T.C*, 295 F.3d 42, 48 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve Board, Bank Holding Companies and Change in Bank Control, "credit bureau services"[13] are "so closely related to banking or managing or controlling banks as to be a proper incident thereto." Since Equifax is a credit bureau and performs credit bureau services, it qualifies as a financial institution for purposes of the GLBA.

31. In order to satisfy their obligations under the GLBA, financial institutions must "develop, implement, and maintain a comprehensive information security program that is (1) written in one or more readily accessible parts, and (2) contains administrative, technical, and physical

[13] Credit bureau services include "[maintaining information related to the credit history of consumers and providing the information to a credit grantor who is considering a borrower's application for credit or who has extended credit to the borrower." See 12 C.F.R. § 225.28

safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue." "See 16 C.F.R. § 314.4. The Code of Federal Regulations States:

> "In order to develop, implement, and maintain [their] information security program, [financial institutions] shall:
>
> (a) Designate an employee or employees to coordinate [their] information security program.
>
> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of [their] operations, including:
>
> (1) Employee training and management;
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks [they] identify through risk assessment, and regularly
>
> (d) Oversee service providers, by:
>
> (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate , safeguards for the customer information at issue; and test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
> (2) Requiring [their] service providers by contract to implement and maintain such safeguards.
>
> (e) Evaluate and adjust [their] information security program in light of the results of the testing and monitoring required by circumstances that [they] know or have reason to know may have a material impact on [their] information security program."

Id.

32. Plaintiffs contend that the ramifications of Defendants' failure to keep Class Members' data secure are severe.

33. The information Defendants lost, including Plaintiffs' identifying information and other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC, *About Identity Theft*, available at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (March 23, 2011).

34. Plaintiffs contend that identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without the owner's permission or consent, in order to commit fraud or other crimes. Plaintiffs' definition of identity theft matches that of the FTC. *Id*.

35. Identity thieves can use identifying data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards. *Id*.

36. Identity thieves can use personal information such as that lost by Defendant and pertaining to the Plaintiffs and other Class Members, which Defendant failed to keep secure by lack of security or failure to implement a more secure system to perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the victims. For instance, identity thieves may commit various types of fraud, including, but not limited to: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

37. Additionally, identity thieves may obtain medical services using the Plaintiffs' lost information or commit any number of other fraudulent activities.

38. Annual monetary losses from identity theft are in the billions of dollars, and Defendant is aware of these staggering statistics.

39. According to a Presidential Report on identity theft, produced in 2008:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts.... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The *President's Identity Theft Task Force Report* at p.21 (Oct. 21, 2008), available at http://www.idtheft.gov/reports/StrategicPlan.pdf.

40. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf.

41. Plaintiffs (and the Class Members seek to represent) now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

42. In addition, under the Interagency Guidelines Establishing Information Security Standards, financial institutions have an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." 12 C.F.R. pt. 225, App. F, The Code of Federal Regulations states:

> "At a minimum, an institution's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;

c. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and

e. Notifying customers when warranted.

Id.

43. Further, the Code of Federal Regulations requires that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, "the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." *Id.*

44. "Nonpublic personal information," includes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, "sensitive customer information" includes PII for purposes of the Interagency Guidelines establishing Information Security Standards.

45. Upon information and belief, Equifax failed to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to: (a) Equifax's failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

46. Upon information and belief, Equifax also failed to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems" as mandated by the GLBA. This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

47. Equifax has also failed to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information, and has failed to communicate directly with Class Members to date.

48. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. §45.

49. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses.[14] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

50. The FTC also has published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[15]

51. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

[14] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
[15] https://www.ftc.gov/news-events/press-releases/2002/01/federal-trade-commission-issues-facts-business-guide-complying

52. By failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

CLASS ACTION ALLEGATIONS

53. Plaintiffs bring all claims individually and as class claims under Federal Rule of Civil Procedure 23(b)(l), (b)(2), (b)(3), and (c)(4).

I. Nationwide Class

54. Plaintiffs bring the negligence, negligence per se claims and Declaratory and Injunctive Relief and other Claims on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> All natural persons and entities in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

II. Utah Subclass

55. Plaintiffs bring the state Data Breach notification claim on behalf of a separate statewide subclass, defined as follows:

> All natural persons and entities in Utah whose personally identifiable information was acquired by unauthorized persons in the Data Breach announced by Equifax on September 7, 2017.

56. Plaintiffs also bring the negligence and negligence *per se* claims (Counts III and IV) separately on behalf of the Utah Subclass, in the alternative to bringing those claims on behalf of the Nationwide Class.

57. Except where otherwise noted, "Class Members" shall refer to members of the Nationwide Class and the Utah Subclass, collectively.

58. Excluded from the Nationwide Class and the Statewide Subclass are Defendants and their current employees, as well as the Court and its personnel presiding over this action.

59. The Nationwide and Statewide Subclass meet the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(l), (b)(2), and (b)(3) for all of the reasons set above.

60. **Numerosity**: The Nationwide and Statewide Subclass are so numerous that joinder of all members is impracticable. Equifax has identified more than 143 million effected customers of the Nationwide Class and Statewide Subclass who may be subject to the Data Breach. The parties will be able to identify each member of the Nationwide Class and Statewide Subclass after Defendants' document production and/or related discovery.

61. **Commonality**: There are numerous questions of law and fact common to Plaintiffs and the Nationwide and Utah Subclasses, including but not limited to the following:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants owed a duty to Plaintiff and Class Members to adequately protect their PII;
- whether Defendant breached its duties to protect the personal information of Plaintiff and Class member;
- whether Defendant knew or should have known that their data security systems and processes were vulnerable to attack;
- whether Plaintiff and Class member suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of PII; and
- whether Plaintiff and Class Members are entitled to equitable relief including injunctive relief.

62. **Typicality**: All Plaintiffs claims are typical of the claims of the Nationwide Class, and each Plaintiffs claims are typical of the claims of the Statewide Subclass.

63. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the Nationwide Class and Statewide Subclasses. Plaintiffs have no interests that are adverse to, or in conflict with, the Class Members. There are no claims or defenses that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient resources to prosecute this action vigorously.

64. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class and

Statewide Subclass predominate over any questions which may affect only individual Class Members in any of the proposed classes, including those listed *supra*.

65. **Superiority**: The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

66. Absent a class action, the majority of Class Members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

67. **Risks of Prosecuting Separate Actions**: Plaintiffs claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(l) because prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Equifax. Equifax continues to maintain the PII of the Class Members and other individuals, and varying adjudications could establish incompatible standards with respect to: Defendants' duty to protect individuals' PII; and whether the injuries suffered by Class Members are legally cognizable, among others. Prosecution of separate actions by individual Class Members would also create a risk of individual adjudications that would be dispositive of the interests of other Class Members not parties to the individual adjudications, or substantially impair or impede the ability of Class Members to protect their interests.

68. **Injunctive Relief**: In addition, Defendants have acted and/or refused to act on grounds that apply generally to the Nationwide and Statewide Subclass, making injunctive and/or declaratory relief appropriate with respect to the classes under Federal Rule of Civil Procedure 23(b)(2). Defendants continue to (1) maintain the PII of Class Members, and (2) fail to adequately protect their PII.

69. **Certification of Particular Issues**: In the alternative, the Nationwide and Statewide Subclass may be maintained as class actions with respect to particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

70. "Once hackers gain access to these key pieces of personal data -- which is akin to the DNA of a person's online digital self -- it is at the cyber thieves' disposal forever to cause harm.[16]" Robb Reck, chief information security officer at Denver-based Ping Identities states, "This opens the door for total identity theft . . .Not only can hackers potentially gain access to victims' financial accounts, such as checking and savings accounts and 401(k)s, and withdraw money, "they can use this information to create a new 'you,' warns Reck. Armed with victims' digital history, hackers can file tax returns using your name and social security number to claim a refund, file fraudulent medical expense claims, attempt to open credit cards, rent an apartment, apply for electric service, get a loan and buy a house in your name without you knowing. "These types of things can bleed over into your life," says former Equifax employee John Ulzheimer. Mr. Ulzheimer advises people to check their credit reports on a "monthly basis," just like balancing a checkbook.

Id.

CAUSES OF ACTION

COUNT I NEGLIGENCE

(On Behalf of the Nationwide Class and the Statewide Subclass)

71. Plaintiffs incorporate paragraphs 1-70 as if set forth in full particularity herein.

72. Equifax owed a duty to Plaintiffs and Class Members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information adequately secured from unauthorized access.

73. Equifax's privacy policy acknowledged Equifax's duty to adequately protect Class Member's PII.

[16] https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/ -"It's very problematic for hackers to have all that important information all in one place," says John Ulzheimer, a credit expert who once worked for Equifax and credit-score firm FICO. "This information is perpetually valuable. You are not going to change your name or date of birth or Social Security number. In five years they will be the same, unlike a credit card that takes five minutes to cancel over the phone."

74. Equifax owed a duty to Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

75. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

76. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class Member's PII.

77. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiffs and Class Members' PII and promptly notify them about the Data Breach.

78. Equifax had a special relationship with Plaintiff and Class Members from being entrusted with their PII, which provided an independent duty of care. Plaintiffs and other Class Members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

79. Equifax's role to utilize and purportedly safeguard Plaintiffs and Class Members' PII presents unique circumstances requiring a reallocation of risk.

80. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Member's PII; and (d) failing to provided adequate and timely notice of the breach.

81. But for Equifax's breach of its duties, Class Member's PII would not have been accessed by unauthorized individuals.

82. Plaintiff and Class Members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class Members.

83. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs and the Nationwide Class Member's PII and consumer reports.

84. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiff and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class Member's PII has also diminished the value of the PII.

85. The damages to Plaintiffs and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

86. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT II

NEGLIGENCE PER SE

(On behalf of the Nationwide Class and the Statewide Subclass)

87. Plaintiffs incorporate paragraphs 1-86 as if fully set forth herein.

88. Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 prohibits "unfair. . .practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by businesses such as Equifax of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form the basis of Equifax's duty.

89. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach in their systems, including specifically the immense damages that would result to consumers.

90. Equifax's violation of Section 5 of the FTC Act constitutes negligence *per se*.

91. Members of the Class and Subclass are within the class of persons Section 5 of the FTC Act was intended to protect as they are individuals engaged in trade and commerce, and bear the risk associated with Defendant's failure to properly secure their PII.

92. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, have put consumers' personal data at unreasonable risk, causing the same harm suffered by Class Members and Subclass Members.

93. Equifax was further required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

94. In order to satisfy their obligations under the GLBA, Equifax was also required to:

"develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue."

16 C.F.R. § 314.4

95. In addition, Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems," pursuant to the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F.

96. Further, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conducted a reasonable investigation to promptly determine the

likelihood that the information has been or will be misused," and "notified the affected customers as soon as possible." *Id*.

97. Equifax violated by GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to: (a) Equifax's failure to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

98. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

99. Equifax also violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

100. Plaintiffs and Class Members were foreseeable victims of Equifax's violations of the FTC Act and GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class Members themselves would cause damages to Class Members.

101. Defendants' failure to comply with the applicable laws and regulations, including the FTC Act and GLBA, constitute negligence *per se*.

102. But for Equifax's violation of the applicable laws and regulations, Class Members' PII would not have been accessed by unauthorized individuals.

103. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiffs and Class Members suffered injury, which includes but is not limited to exposure to a

heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class Members' PII has also diminished the value of the PII.

104. The damages to Plaintiffs and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of it's the applicable laws and regulations, especially since this is not the first Data Breach Equifax has experienced.

105. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT III

VIOLATION OF THE UTAH UNFAIR COMPETITION LAW UCA §13-5a-103, ET SEQ.

106. Plaintiffs incorporate by reference paragraphs 1-105 as if fully set forth herein.

107. Defendants' conduct constitutes unfair and illegal and fraudulent business practices within the meaning of the Utah Unfair Competition Law.

108. Defendants' conduct violated certain laws as alleged herein, and, *ergo*, by engaging in the said conduct in the course of doing business, Defendants engaged in unlawful business practices in violation of the Utah Unfair Competition Law, Utah Code Annotated (UCA) § 13-5a-101 *et seq*.

109. Plaintiffs contend that by engaging in the above-described conduct in the course of doing business, Defendants engaged in unfair business practices in violation of the Utah Unfair Competition Law (U.C.A. § 13-5a-101 *et seq*). The harm and potential harm to each Plaintiff outweighed any utility that Defendants' conduct may have produced.

110. Plaintiffs contend that Defendant Equifax's failure to disclose information concerning the Data Breach directly and promptly to affected customers, constitutes a fraudulent act or practice in violation of Utah Unfair Competition Laws.

111. Plaintiffs suffered injury in fact and lost property and money as a result of Defendants' joint conduct, or lack to institute appropriate protections and safeguards.

112. Plaintiffs seek restitution and injunctive relief on behalf of the Class.

COUNT IV

INVASION OF PRIVACY- INTRUSION, PUBLIC DISCLOSURE OF PRIVATE FACTS, MISAPPROPRIATION OF LIKENESS AND IDENTITY, UTAH CONSTITUTIONAL RIGHT TO PRIVACY

113. Plaintiffs incorporate by reference paragraphs 1-112 as if set forth in full particularity herein.

114. Plaintiffs had a reasonable expectation of privacy in the private information Defendants mishandled and/or failed to protect.

115. By failing to keep Plaintiffs private information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants invaded Plaintiffs privacy by:

a. intruding into Plaintiffs private affairs in a manner that would be highly offensive to a reasonable person;
b. publicizing private facts about Plaintiffs, which is highly offensive to a reasonable person;
c. using and appropriating Plaintiffs identity without Plaintiffs' consent; and,
d. violating Plaintiffs right to privacy under Utah Constitution, Article 1, Section 1, as well as the privacy provisions from other States, through the improper use of Plaintiffs' private information properly obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

116. Plaintiffs allege that Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs position would consider Defendants' actions highly offensive.

117. Plaintiffs assert that Defendants invaded Plaintiffs right to privacy and intruded into Plaintiffs private affairs by misusing and/or disclosing Plaintiffs private information without their informed, voluntary, affirmative and clear consent.

118. Plaintiffs allege that Defendant had knowledge of superior security but chose not to implement said superior security for financial gain, and thereby exposed Plaintiffs to added, unnecessary risk.

119. Plaintiffs contend that as a direct and proximate result of such misuse and disclosures, Plaintiffs reasonable expectations of privacy in their private information was unduly frustrated and thwarted, and that the Defendants' conduct amounted to a serious invasion of Plaintiffs' protected privacy interests.

120. Plaintiffs assert Defendants had a duty to protect Plaintiffs private information and that in failing to protect Plaintiffs private information, and in misusing and/or disclosing Plaintiffs private information, Defendant has acted with malice, oppression and in conscious disregard of Plaintiffs and the Class Members' rights to have such information kept confidential and private. Plaintiffs, accordingly, seek an award of punitive damages on their behalf as well as on behalf of the Class Members.

COUNT V

BREACH OF CONTRACT AND BALIMENT

121. Plaintiffs incorporate by reference paragraphs 1-120 as if set forth with full particularity herein.

122. Plaintiffs and the Class Members delivered and entrusted their PII to Defendant for the sole purpose of receiving secure services from Defendant.

123. Plaintiffs allege that Equifax made representations and entered into contractual and implied contractual relations regarding Equifax's duty to safeguard Plaintiffs PII.

123. Plaintiffs contend that the contractual duties between Plaintiffs and Defendant were established via representations and a pattern of conduct between Equifax and its customers, as well as established by business and governmental agencies in their contracts with their clients.

124. Plaintiffs assert that Equifax breached its duty to safeguard its customers' privacy, and thereafter intentionally failed to inform Plaintiffs and Class Members of the Data Breach.

125. The Utah Supreme Court has held that breach of contract, standing alone, does not call for punitive damages even if intentional and unjustified, but such damages are allowable if there is some independent tort indicating malice, fraud or wanton disregard for the rights of others. *Hal Taylor Assocs v. Unionamerica, Inc.*, 657 P.2d 743, 750 (Utah 1982); s*ee also Dold v. Outrigger Hotel, 501 P.2d 368 (1972)*; *Temmen v. Kent-Brown Chevrolet Co., 605 P.2d 95 (1980)*; *Jackson v. Glasgow, 622 P.2d 1088 (1980).* Plaintiffs contend that Equifax's actions, after it became aware of the Data Breach on July 29, 2017, are demonstrative of malfeasance, fraud and wanton disregard for the rights of others, as demonstrated by the fact that is officers sold over 685,000 shares of stock on August 1, 2017, prior to notifying the public of the Data Breech. Plaintiffs contend that coupled with its failure to act in response to Data Breech it allowed its officers to engage in illegal insider trading, calling for punitive damages.

126. Plaintiffs contend that the wanton refusal to notify customers of the data breach, until the breach was identified by a third party, warrants the imposition of punitive damages against the Defendants pursuant to the independent intentional torts committed by the Defendants.

127. Plaintiffs additionally contend that during the time of bailment, Defendants owed Plaintiffs and the Class Members a duty to safeguard their information properly and maintain reasonable security procedures and practices to protect such information.

128. Plaintiffs allege that as a result of these breaches of duty, breach of contract, and breach of bailment, Plaintiffs and the Class Members have suffered harm.

129. Plaintiffs seek actual damages from all Defendants on behalf of the Class.

COUNT VI

CONVERSION

130. Plaintiffs incorporate by reference paragraphs 1-129 as if set forth with full particularity herein.

131. Plaintiffs and Class members were the owners and possessors of their private information. As the result of Defendants' wrongful conduct, Defendants have interfered with the Plaintiffs and Class Members' rights to possess and control such property, to which they had a superior right of possession and control at the time of conversion.

132. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class Members suffered injury, damage, loss or harm and therefore seek compensatory damages.

133. Plaintiffs allege that in converting Plaintiffs PII, Defendants have acted with malice, oppression and in conscious disregard of the Plaintiffs and Class Members' rights. Plaintiffs, accordingly, seek an award of punitive damages on behalf of the Class Members.

134. Plaintiffs and the Class members did not consent to Defendants' mishandling and loss of their PII.

COUNT VII

VIOLATION OF UCA § 13-44-102

135. Plaintiffs incorporate by reference paragraphs 1-134 as if set forth with full particularity herein.

136. The data breach described above constituted a "breach of the security system" of Equifax, within the meaning of Section 13-44-102, Utah Code Annotated and constituted a breach of Equifax's announced adequate security measures.

137. The information lost in the data breach constituted PII within the meaning of Section 13-44-102(3)(a) Utah Code Annotated.

138. Plaintiffs contend that Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach, which failure caused Plaintiffs and other Class Members harm and injury.

139. Plaintiffs assert that Equifax unreasonably delayed informing anyone about the breach of security of Plaintiffs and Class Members' confidential and non-public information after Defendant Equifax knew the data breach had occurred.

140. Plaintiffs allege Defendant failed to disclose to Plaintiffs and Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, personal information when Equifax knew, or reasonably believed such information had been compromised.

141. Upon information and belief, no law enforcement agency instructed Equifax that notification to Plaintiffs or Class Members would impede investigation.

142. Plaintiffs allege that as a result of Defendant's breach of contract, negligence, failure to secure PII, Plaintiffs and other Class Members incurred economic damages, including, but not limited to, expenses associated with necessary credit monitoring.

143. Plaintiffs, individually and on behalf of the Class Members, seek all remedies available under applicable Utah and Federal laws, including, but not limited to: (a) damages suffered by Class members as alleged above; (b) statutory damages jointly and severally for Defendants' willful, intentional, and/or reckless violation of Utah Unfair Competition Act; and (c) equitable relief.

204. Plaintiffs, individually and on behalf of the Class Members, also seek reasonable attorneys' fees and costs as allowed by statue, and law.

INJUNCTIVE RELIEF

145. Plaintiffs request, on behalf of themselves and Class Members – that (a) Equifax be compelled to notify Class Members of the Data Breach under the common law, Section 5 of the FTC Act and GLBA; (b) the Court hold that Equifax breached and continues to breach this legal duty by failing to employ reasonable security measures to secure Class Members' PII; (c) the Court hold that Equifax's breach of its legal duty proximately caused the Data Breach; (d) the Court hold that Equifax's continued failure to disclose exactly the scope of the Data Breach, and the individuals affected by the breach makes it impossible for Class Members to take appropriate measures to mitigate the risk of future identity theft.

146. The Court also should issue corresponding injunctive relief requiring Equifax to employ adequate security protocols to protect the PII of Class Members in its possession. Specifically, this injunction should, among other things direct Equifax to:

(a) utilize industry standard secure default password and pin combinations in protecting individuals' PII;

(b) consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

(c) audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

(d) regularly test its system for security vulnerabilities, consistent with industry standards; and,

(e) immediately notify all Class Members of the data breach, and the scope of PII that was disclosed.

147. If an injunction is not issued, Class Members will suffer irreparable injury and lack an adequate remedy in the event of another data breach, at Equifax. The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

148. The hardship to the Class, if an injunction does not issue, exceeds the hardship to Equifax if an injunction is issued. Among other things, if another data breach occurs at Equifax, the class will likely incur further risk of identity theft and fraudulent use of their PII. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security and notice measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

149. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Equifax, thus eliminating the injuries that would result to Class Members and others whose PII Equifax later obtains whose information would be compromised.

RELIEF REQUESTED

Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter judgment against Equifax as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and Subclass requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Class and Subclass requested herein;

B. Injunctive relief requiring Defendants Equifax, Inc. and Equifax Information Services, LLC, to (1) strengthen their data security systems that maintain PII to comply with the, the

applicable state laws alleged herein and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

C. An order requiring Defendants to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiff and all Class (and Subclass) Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial, but not less than $5,000,000,000.00;

E. An award to Plaintiffs and all Class (and Subclass) Members of credit monitoring and identity theft protection services;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity;

H. Punitive damages; and

I. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial of their claims to the extent authorized by law.

Dated: September 11, 2017

Christensen Young & Associates, PLLC

__/s/ Steven A. Christensen___.

Steven A. Christensen
Christensen Young & Associates, PLLC
9980 So. 300 West, #200
Sandy, Utah, 84070
(801) 676-6447
steven@christensenyounglaw.com